What's the Best Way to Back Up My Computer?

Mar 23, 2023

A little bit of preparation now will save you a massive headache later.

Corbin Davenport / How-To Geek

Key Takeaways

We recommend backing up your computer in multiple ways so you have both an onsite and an offsite backup. You can back up to an external drive, use an online backup service, back up to a NAS over your local network, or even try a cloud storage service.

Everyone loses data at some point in their lives. Your computer's hard drive could fail tomorrow, ransomware could hold your files hostage, or a software bug could delete your important files. If you're not regularly backing up your computer, you could lose those files forever.

Backups don't have to be hard or confusing, though. You've probably heard about countless different backup methods, but which one is right for you? And what files do you really need to back up?

Which Files Should You Back Up?

You need to back up your personal data---the files that are irreplaceable that are stored on your PC or Mac. You can always reinstall your operating system and redownload your programs if your hard drive fails, but your own personal data is irreplaceable. (On Windows 10 and Windows 11, you can "Reset" your operating system to quickly get a fresh system.)

Any personal documents, photos, home videos, and any other data on your computer should be backed up regularly. Those can never be replaced. If you've spent hours painstakingly ripping audio CDs or video DVDs, you may want to back those files up, too, so you don't have to do all that work over again.

Your operating system, programs, and other settings can also be backed up. You don't have to back them up, necessarily, but it can make your life easier if your entire hard drive fails. If you're the type of person that likes to play around with system files, edit the registry, and regularly update your hardware, having a full system backup may save you time when things go wrong.

What's the Best Way to Back Up a Computer?

There are many ways to back up your data, from using an external drive to backing up those files on a remote server over the Internet. Here are the strengths and weaknesses of each:

Back Up to an External Drive

If you have an external USB hard drive, you can just back up to that drive using your computer's built-in backup features. On Windows 10 and Windows 11, use File History. On Macs, use Time Machine.

Occasionally connect the drive to the computer and use the backup tool, or leave it plugged in whenever you're home, and it'll back up automatically.

Pros: Backing up is cheap and fast.

Cons: If your house gets robbed or catches on fire, your backup can be lost along with your computer, which is very bad.

Back Up Over the Internet

If you want to ensure your files stay safe, you can back them up to the internet with an online backup service like Backblaze. Backblaze is our favorite online backup service, and we have recommended it ever since CrashPlan decided to no longer serve home users. There are also other solid options, like IDrive and Carbonite Safe.

For a low monthly fee (about $5 to $7 a month), these programs run in the background on your PC or Mac, automatically backing up your files to the service's web storage. If you ever lose those files and need them again, you can restore them.

Pros: Online backup protects you against any type of data loss---hard drive failure, theft, natural disasters, and everything in between.

Cons: These services usually cost money, and the initial backup can take much longer than it would on an external drive--especially if you have a lot of files. Restoring a backup can take a while, too.

Back Up to a NAS on Your Network

To create backups and store them locally, you don't have to plug an external hard drive into all the computers you use. You can get a NAS (network-attached storage) device instead. All the computers on your home network can back up and restore from the NAS.

NAS devices may also have other features, like the ability to run a Plex media server for networked media streaming or integrate with Apple Time Machine for seamless backups from Macs, too.

Pros: A NAS lets you back up multiple devices to one central location on your network. It will be faster than backing up online.

Cons: Like with backing up to an external drive, you will lose your backups along with your computers if you experience a robbery, fire, or similar event where you lose your electronics. For backing up a single computer, an external hard drive will be faster and cheaper.

Use a Cloud Storage Service

Backup purists will say this isn't technically a backup method, but for most people, it serves a similar enough purpose. Rather than just storing your files on your computer's hard drive, you can store them on a tool like Dropbox, Google Drive, Microsoft OneDrive, or a similar cloud storage service.

The service you choose will then automatically sync to your online account and to your other PCs. If your hard drive dies, you'll still have the copies of the files stored online and on your other computers.

Pros: This method is easy, fast, and in many cases, free, and since it's online, it protects you against all types of data loss.

Cons: Most cloud services only offer a few gigabytes of space for free, so this only works if you have a small number of files you want to back up, or if you're willing to pay for extra storage. Depending on the files you want to back up, this method can either be simpler or more complicated than a straight-up backup program.

Online Backup Service vs. Cloud Storage

While backup programs like Backblaze and cloud storage services like Dropbox are both online backups, they work in fundamentally different ways. Dropbox is designed to sync your files between PCs, while Backblaze and similar services are designed to backup large amounts of files. Backblaze will keep multiple copies of different versions of your files, so you can restore the file exactly as it was from many points in its history. And, while services like Dropbox are free for small amounts of space, Backblaze's low price is for as big a backup as you want. Depending on how much data you have, one could be cheaper than the other.

Backblaze does have one big limitation you should keep in mind. If you delete a file on your computer, it will be deleted from your online backups after 30 days. You can't go back and recover a deleted file or the previous version of a file after this 30-day period. Other online backup services usually work similarly; be sure to check an online backup service's information for more details. So be careful when deleting those files if you might want them back!

Why You Need Multiple Backup Methods

So which should you use? Ideally, you'd use at least two of them. Why? Because you want both offsite and onsite backups.

"Onsite" literally means backups stored at the same physical location as you. So, if you back up to an external hard drive and store that at home with your home PC, that's an onsite backup.

Offsite backups are stored at a different location. So, if you back up to an online server, like Backblaze or Dropbox, that's an offsite backup.

Onsite backups are faster and easier, and they should be your first line of defense against data loss. If you lose files, you can quickly restore them from an external drive. But you shouldn't rely on onsite backups alone. If your home burns down or all the hardware in it is stolen by thieves, you'd lose all your files.

Offsite backups don't have to be a server on the Internet, either, and you don't have to pay a monthly subscription for one. You could back up your files to a hard drive and store it at your office, at a friend's house, or in a bank vault, for example. It'd be a bit more inconvenient, but that's technically an offsite backup.

Similarly, you could also store your files in Dropbox, Google Drive, or OneDrive and performing regular backups to an external drive. Or you could use Backblaze to back up online and Windows File History to create a local backup. There are a lot of ways to use these services in tandem, and it's up to you how to do it. Just make sure you have a solid backup strategy, with onsite and offsite backups, so you have a wide safety net against ever losing your files.

You should also consider having an offline backup---just in case.

Related: You're Not Backing Up Properly Unless You Have Offsite Backups

Why You Need to Automate Your Backups

All that may sound complicated, but the more you automate your backup system, the more frequently you'll be able to back up, and the greater the odds you'll stick with it. That's why you should use an automated tool instead of copying files to an external drive by hand. You can just set it up once and forget it.

That's one reason we really like online services like Backblaze. If it's backing up to the internet, it can automatically do that every single day. If you have to plug in an external drive, you have to put in more effort, which means you'll back up less often, and you may eventually stop doing it. Keeping everything automatic is well worth the price.

If you don't want to pay anything and want to primarily rely on local backups, consider using a file-syncing service like Dropbox, Google Drive, or Microsoft OneDrive to synchronize your important files online. That way, if you ever lose your local backup, you'll at least have an online copy.

Ultimately, you just need to think about where your files are and ensure you have multiple copies at all times. Ideally, those copies should be in more than one physical location. As long as you're actually thinking about what you'll do if your computer dies, you should be way ahead of most people.

About The Author

Chris Hoffman is the former Editor-in-Chief of How-To Geek. Chris has personally written over 2,000 articles that have been read more than one billion times---and that's just here at How-To Geek.

With over a decade of writing experience in the field of technology, Chris has written for a variety of publications including The New York Times, Reader's Digest, IDG's PCWorld, Digital Trends, and MakeUseOf. Beyond the web, his work has appeared in the print edition of The New York Times (September 9, 2019) and in PCWorld's print magazines, specifically in the August 2013 and July 2013 editions, where his story was on the cover. He also wrote the USA's most-saved article of 2021, according to Pocket.

Chris was a PCWorld columnist for two years. He founded PCWorld's "World Beyond Windows" column, which covered the latest developments in open-source operating systems like Linux and Chrome OS. Beyond the column, he wrote about everything from Windows to tech travel tips.

The news he's broken has been covered by outlets like the BBC, The Verge, Slate, Gizmodo, Engadget, TechCrunch, Digital Trends, ZDNet, The Next Web, and Techmeme. Instructional tutorials he's written have been linked to by organizations like The New York Times, Wirecutter, Lifehacker, the BBC, CNET, Ars Technica, and John Gruber's Daring Fireball. His roundups of new features in Windows 10 updates have been called "the most detailed, useful Windows version previews of anyone on the web" and covered by prominent Windows journalists like Paul Thurrott and Mary Jo Foley on TWiT's Windows Weekly. His work has even appeared on the front page of Reddit.

Articles he's written have been used as a source for everything from books like Team Human by Douglas Rushkoff, media theory professor at the City University of New York's Queens College and CNN contributor, to university textbooks and even late-night TV shows like Comedy Central's @midnight with Chris Hardwick.

Starting in 2015, Chris attended the Computer Electronics Show (CES) in Las Vegas for five years running. At CES 2018, he broke the news about Kodak's "KashMiner" Bitcoin mining scheme with a viral tweet. A wave of negative publicity ensued, with coverage on BuzzFeed News, CNBC, the BBC, and TechCrunch. The company's project was later reportedly shut down by the U.S. Securities and Exchange Commission.

In addition to his extensive writing experience, Chris has been interviewed as a technology expert on TV news and radio shows. He gave advice on dark web scans on Miami's NBC 6, discussed Windows XP's demise on WGN-TV's Midday News in Chicago, and shared his CES experiences on WJR-AM's Guy Gordon Show in Detroit.

Chris also ran MakeUseOf's email newsletter for two years. Nearly 400,000 subscribers received the newsletter complete with a handwritten tip every day.

Get around this BSOD error on your PC.